

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-against-

NICHOLAS TARTAGLIONE,

Defendant.

:
:
:
:
:
:
:

16-CR-832 (KMK)

MEMORANDUM OF LAW
IN SUPPORT OF MOTION TO SUPPRESS CELL PHONE TRACKING DATA

**BARKET EPSTEIN KEARON
ALDEA & LOTURCO, LLP**
666 Old Country Road, Suite 700
Garden City, New York 11530
Ph: (516) 745-1500
F: (516) 745-1245

INTRODUCTION

In *Carpenter v. United States*, 138 S. Ct. 2206, 2216-17 (2018), the Supreme Court held that when the government turns a suspect's cell phone into a tracking device without a warrant, it violates the Fourth Amendment. In this case, the government obtained cell site location information ("CLSI") for Mr. Tartaglione's cell phone without a warrant. In the process, it unquestionably violated his rights under the Fourth Amendment. Thus, this data must be suppressed unless the "good faith" doctrine applies. Here, that doctrine – which is designed to prevent paradoxical circumstances in which the government would be penalized for relying upon settled precedent that was later overturned – is inapplicable for two reasons.

First, in violating Mr. Tartaglione's rights under the Fourth Amendment, the government acted under the Stored Communications Act (the "SCA"). However, the plain text of the SCA barred the very conduct for which the government used it as a springboard. As this Court and others had held years prior to the warrantless data-retention in issue, the SCA allows for the recovery of a vast array of information, but not location-data from tracking devices like cell phones. Thus, this is not a classic "good faith" case in which the government violated a suspect's constitutional rights by reasonably relying upon a statute. This is a case in which the government violated a suspect's constitutional rights by relying upon a statute that *also* prohibited the same conduct.

Second, at the time that the government obtained Mr. Tartaglione's phone-tracking data in 2016, federal courts sitting in New York were already "split" on whether government agents could seize phone-tracking data without a warrant, with cases in the

Southern District explicitly holding that this was impermissible, the Supreme Court of the United States strongly suggesting that these types of intrusions would require a warrant (see *United States v. Jones*, 565 U.S. 400 [2012]), and a raging controversy brewing throughout the country on this issue. In this landscape, it cannot be said that the government acted in “good faith” in failing to obtain a warrant – as it regularly does when it seeks private information in other contexts – and gambling that case-law developments would ultimately prove a warrant unnecessary. When the government eschews constitutional caution for such aggression, the decision is not risk-free. Far from imposing appreciable deterrence, as is the aim of the exclusionary rule, a contrary holding would encourage future law enforcement officials to exploit legal splits rather than be cautioned by them.

For these reasons, choosing a course that was contrary to both the plain terms of the statute upon which it relied, and to case law in this Court, and at a time when these issues were at the forefront of a raging legal debate about the very conduct the government was contemplating, the government’s failure to obtain a warrant in this capital case should not be shielded by the good faith doctrine.

The statutory analysis is unaltered by recent Second Circuit precedent, like *United States v. Zodhiates*, 901 F.3d 137 (2d Cir. 2018), applying the good faith doctrine to deny suppression of a 2011 pre-*Carpenter* warrantless seizure of CSLI. *Zodhiates* did not analyze the “good faith” question in terms of the statutory language of the Stored Communications Act, or in terms of the case law existing in New York federal courts in 2016 construing this language as barring the warrantless recovery of cell-site data. Thus,

because it did not consider or address the issues raised here, *Zodhiates* does not control the outcome in this case.¹

In sum, the government cannot show “good faith” in engaging in conduct that, at that time, violated federal statutory law, ran contrary to decisional law from this Court and the weight of authority from numerous other circuits, and which was shortly thereafter recognized by the Supreme Court as a violation of the Fourth Amendment, as a natural extension of the logic in its prior holdings. While law enforcement should not be penalized for following settled precedent, neither should it be rewarded for exploiting greying areas of constitutional law before they fade to black. The appropriate remedy for the Fourth Amendment violation here is suppression.

FACTUAL AND LEGAL BACKGROUND

By the middle of this decade, a fight was already raging among federal courts sitting in New York about the government’s ability to track people’s cell phones without a warrant. *See, e.g., Cucuta v. New York City*, 25 F. Supp.3d 400, 416 (S.D.N.Y. 2014) (“the decisions in this District and the Eastern District of New York are split as to whether police need a search warrant for cell site location information”).

In June 2016, the government in this case sought an order to peruse the call-data from every phone, from every major cell-service provider, for every person who called or received a call using a cell-tower that serviced 69 Brookside Avenue in Chester, New York. *See* Exhibit A, at para. 2(a) (seeking records of “any wireless telephone call” from “AT&T, SPRINT/NEXTEL, T-MOBILE, METRO PCS and VERIZON WIRELESS”). This application implicated the records of tens of thousands of calls in and around

¹ And, to the extent that this Court does deem this Second Circuit case law binding, the defense asserts, for purposes of preservation, that it was wrongly decided.

Chester, and was granted the same day (*see* Exhibits A and B); but it was not targeted at any particular phone and did not seek tracking data.

During this time, the legal controversy over cell-data had reached a fever pitch. *See, e.g.,* Ilya Shapiro and Jim Harper, *The Fourth Amendment Protects Your Cell-Location Data*, CATO INSTITUTE (Aug. 28, 2016);² Judge Herbert B. Dixon Jr., *Telephone Technology versus the Fourth Amendment*, AMERICAN BAR ASSOCIATION (May 1, 2016);³ Paul Cividanes, *Cellphones and the Fourth Amendment: Why Cellphone Users Have a Reasonable Expectation of Privacy in their Location Information*, 25 J. OF LAW AND POLICY 317 (2016).⁴ *See also* Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY LAW JOURNAL 527 (2017).⁵ Adding to the noise, in April 2016, the Sixth Circuit decided *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016)—a case that was soon slated for review in the Supreme Court to resolve, once and for all, whether the warrantless intrusion into people’s location information breached the Fourth Amendment.

Before the cacophony cleared, the United States Attorney’s Office returned ten days later in June 2016 with another application for phone records. This time, the application was narrower in focus but broader in implication: while it sought records emanating from only five phone numbers, it sought data to track these phones—cell service location information, or “CSLI”—for their movements over the course of more

² Available at: <https://www.cato.org/blog/fourth-amendment-protects-cell-location-data>.

³ Available at: https://www.americanbar.org/groups/judicial/publications/judges_journal/2016/spring/telephone_technology_versus_the_fourth_amendment/.

⁴ Available at: <https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1526&context=jlj>.

⁵ Available at: http://law.emory.edu/elj/_documents/volumes/66/3/levinson-waldman.pdf.

than a year and a half. In the application’s words, it sought “all available historical cell site location information” showing cell towers and sectors that routed “any phone, text, or data communication to or from the cellphone[s],” including the “approximate range of the target phone from the cell towers” during the time period ranging from “January 1, 2015 through the date of this Orders....” *See* Exhibit C, at ¶2.

Despite the cresting wave in this area of Fourth Amendment jurisprudence, these applications never alleged “probable cause,” did not ask for a search warrant, and reserved any acknowledgment of the central legal controversy to a footnote. *See* Exhibit C, at 2-3 (fn. 2).

Even there, the government did not mention *Cucuta v. New York City*, 25 F. Supp.3d 400 (S.D.N.Y. 2014), decided just two years earlier, and recognizing the split of authority among local federal courts. Nor did it mention *In re Application of U.S. for an Order Authorizing Use of a Pen Register with Caller Identification Device Cell Site Location Auth. on a Cellular Tel.* (“*In re Application of U.S.*”), 2009 WL 159187 (S.D.N.Y. 2009)—also decided in this Court, containing a comprehensive analysis of CSLI, and concluding that tracking-data is unrecoverable as a matter of federal statutory law.

And the government’s application did not discuss *United States v. Jones*, 565 U.S. 400 (2012). While *Jones* involved the GPS-tracking of a car, and was ultimately decided as a matter of physical trespass, five Justices on the Supreme Court agreed that long-term tracking of one’s physical movements caused friction with Fourth Amendment expectations of privacy. *Id.* at 415-16; 429-30. Last year, the Second Circuit held that *Jones* did not have clear enough application to CSLI to trigger the exclusionary rule.

United States v. Chambers, 751 F. App'x 44, 46-47 (2d Cir. 2018). But *Chambers* was still two years away from being decided when the government filed the applications in issue here. And with *Jones* firmly on the books, the government did not seek to distinguish it or otherwise claim its inapplicability to CSLI. Instead, the applications simply do not cite *Jones* at all.

With this gloss on the applications, the orders for tracking-data were again granted. See Exhibit D. And without a warrant or a discussion of probable cause, 18 months' worth of cell phone tracking information came into the government's grasp.

ARGUMENT

THE COURT SHOULD SUPPRESS THE CSLI RECOVERED FROM MR. TARTAGLIONE'S CELL PHONES WITHOUT A WARRANT, BECAUSE THE RETENTION VIOLATED TARTAGLIONE'S RIGHTS UNDER THE FOURTH AMENDMENT AND FEDERAL STATUTORY LAW, AND THE GOVERNMENT LACKS "GOOD FAITH" TO AVOID THE EXCLUSIONARY RULE.

"Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection." *Carpenter v. United States*, 138 S. Ct. 2206, 2216-17 (2018). "Whether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier, ... an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI." *Id.* at 2217.

"As with GPS information," after all, "the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Id.*

(quoting Sotomayor, J., concurring in *United States v. Jones*). CSLI records, in other words, “hold for many Americans the privacies of life.” *Id.* (internal quotations omitted).

Even worse than GPS monitoring of a vehicle, “a cell phone—almost a feature of human anatomy—tracks nearly exactly the movements of its owner.” *Id.* (internal quotation omitted). “While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time,” such that a cell phone “faithfully follows its owner beyond public thoroughfares and into private residences, doctor’s offices, political headquarters, and other potentially revealing locales.” *Id.* at 2218.

Because Americans have a reasonable expectation of privacy in this CSLI—and because the government’s perusal of such records is thus a search under the Fourth Amendment—“the Government must generally obtain a warrant supported by probable cause before acquiring such records.” *Carpenter*, 138 S. Ct., at 2221.

Here, as in *Carpenter*, the government “acquired the cell-site records pursuant to a court order issued under the Stored Communications Act,⁶ which required the Government to show ‘reasonable grounds’ for believing that the records were ‘relevant and material to an ongoing investigation;’” however, “[t]hat showing falls well short of the probable cause required for a warrant.” *Id.* The retrieval of Tartaglione’s phone-tracking data without a search warrant was, thus, a violation of his rights under the Fourth Amendment.

Nevertheless, the government will surely argue that suppression is an inappropriate remedy because law enforcement obtained Tartaglione’s CSLI in “good faith.” Under federal case law, the exclusionary rule is not an automatic remedy to victims of Fourth Amendment violations. It is meant to impose “appreciable deterrence”

⁶ See, e.g., Exhibit C, at ¶2 (seeking the orders “pursuant to the Stored Communications Act”).

against government agents engaging in wrongdoing, *Herring v. U.S.*, 555 U.S. 135, 141 (2009), and, thus, exclusion remains on the sidelines when such agents have acted with an “objectively reasonable good-faith belief that their conduct was lawful.” *United States v. Zodhiates*, 901 F.3d 137, 144 (2d Cir. 2018) (internal references omitted).

One way “good faith” emerges, as in issue here, is when the government acts in “objectively reasonable reliance” on appellate precedent of the Second Circuit or the Supreme Court. *United States v. Agular*, 737 F.3d 251, 261 (2d Cir. 2013). The government will argue it obtained Tartaglione’s CSLI in good faith because, until *Carpenter*, it could rely upon the “third party doctrine” to believe that Americans lacked Fourth Amendment rights over their phone-tracking data. *See* Exhibits C, at fn. 2 (making this argument).

As set forth below, this resort to good faith is ultimately unpersuasive on the facts of this case. When the government obtained Tartaglione’s CSLI, the relationship between the third party doctrine and CSLI was already the subject of sharp constitutional dispute; and, more directly, the third party doctrine was, and is, irrelevant to the statutory blockades that prevented the government from obtaining this data without a warrant in the first place. For these reasons, suppression should now be granted.

A. The Government Lacked Good Faith, Because It Relied Upon Statutory Law that Barred the Recovery of the Records in Issue.

The government obtained Tartaglione’s tracking-data pursuant to an order under the Stored Communications Act, 18 U.S.C. §2701 *et seq.* (the “SCA”). In particular, the SCA allowed the government to “require a provider of electronic communication service” to disclose “a record or other information pertaining to a subscriber”—but only

when, as relevant, it obtained a warrant on probable cause or a court order on reasonable suspicion. *See* 18 U.S.C. §2703(c)(1). The government obtained the CSLI tracking-data through an order on reasonable suspicion, and thus claimed compliance with the SCA.

The problem is, as this Court recognized long before the government’s actions in this case, “the SCA sets movement/location information outside its scope[.]” *In re Application of U.S.*, 2009 WL 159187, at *3 (S.D.N.Y. 2009). The SCA governs companies to the extent they are servicing an “electronic communication,” but, as set forth in Title 18, an “electronic communication ... does not include ... any communication from a tracking device....” *See* 18 U.S.C. §2510(12).

As early as 2009—and certainly by 2016—modern technology had advanced far enough that “a cell phone f[ell] squarely within the statutory definition of the term ‘tracking device.’” *In re Application of U.S.*, at *3 (finding this conclusion “inescapable”). And thus, statutorily, **“since all communications from a tracking device are exempt from disclosure under the SCA, no order issued pursuant to section 2703(d) [on reasonable suspicion] can authorize disclosure of CSLI.”** *Id.* (emphasis added). *See also In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 534 F. Supp.2d 585 (W.D. Pa. 2008) (noted in *In re Application of U.S.* for its “excellent summary of the relevant opinions [on the topic]”); *In re Application of U.S. for an Order Authorizing Disclosure of Location Info. Of a Specified Wireless Tel.*, 849 F. Supp.2d 526, 576-78 (D. Md. 2011). *But see In re Application of U.S. for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 460 F. Supp.2d 448 (S.D.N.Y. 2006) (decided prior to *In re*

Application of U.S., and coming to a different conclusion—one that relies upon the notion that the Court should not “incorporate the term ‘electronic communication’ into the term ‘electronic communications service’”).

The very existence of *In re Application of U.S.*, and of its sister case law, shows that the government could not have had “objectively reasonable reliance”⁷ on appellate precedent for its warrantless seizure of Tartaglione’s CSLI. Nor could it have had “objectively reasonable reliance on [the] statute.” *Illinois v. Krull*, 480 U.S. 340 (1987). Such clear appellate precedent or statutory text would have made these decisions gratuitous. And indeed, if the government truly thought *In re Application of U.S.* were inapplicable, it had a way to express that good faith: it could have explained its reasoning to the issuing Judge, rather than ignoring the case altogether, which is what it did.

In *Zodhiates*, the Second Circuit held that, before *Carpenter*, the government could in good faith assume its warrantless retrieval of CSLI passed muster under the Fourth Amendment. 901 F.3d 137, 143-44 (2d Cir. 2018). However “*stare decisis* ... does not constrict the court when considering new arguments not raised in the prior relevant proceeding.” *Sears Petroleum & Transport Corp. v. Archer Daniels Midland Co.*, 2007 WL 2156251, at *12 (N.D.N.Y. 2007). Regardless of Fourth Amendment questions, and thus regardless of *Zodhiates*, the government’s seizure of CSLI was prohibited by the express text of the SCA – an argument that the Second Circuit did not consider in *Zodhiates*. Since the government’s silent spurn of this text was not “objectively reasonable,” and since exclusion would thus carry “appreciable deterrence,”

⁷ *United States v. Aguilar*, 737 F.3d 251, 261 (2d Cir. 2013).

Herring v. U.S., 555 U.S. 135, 141 (2009), the government’s resort to good faith should be rejected.

Because the plain statutory text of the SCA barred recovery of Tartaglione’s CSLI, the government cannot show the appropriate good faith to avoid the exclusionary rule. Suppression should be granted.

B. The Government Lacked Good Faith, Because It Relied upon Constitutional Law that Already Barred the Conduct in Issue; To the Extent the *Zodhiates* or *Chambers* have Held Otherwise, they Were Wrongly Decided.⁸

In 2012, five Justices on the Supreme Court signaled that the long-term tracking of United States residents hit Fourth Amendment tripwires. As Justice Sotomayor framed the problem in the (parallel) context of GPS tracking:

Awareness that the Government may be watching chills associational and expressive freedoms. And the Government’s unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion chooses to track—may alter the relationship between citizen and government in a way that is inimical to democratic society. I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one’s public movements.

See United States v. Jones, 565 U.S. 400, 415-16 (2012) (Sotomayor, J., concurring)

(internal references omitted, and separate paragraphs merged).

⁸ The defense acknowledges that this Court is bound by this facet of *Zodhiates* and *Chambers* – though not by their ultimate holdings (*see supra*, point A) – and asserts this argument for the sake of appellate preservation.

Or in the words of Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan in the same case: “the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. ... We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.” *Id.* at 429-30 (Alito, J., concurring).

The government in this case will claim its warrantless intrusion into Tartaglione’s CSLI was in good faith because the SCA was not “clearly unconstitutional,” *Illinois v. Krull*, 480 U.S. 340 (1987), and thus its reliance on SCA procedures sprouted from “objectively reasonable” reliance upon settled law. *United States v. Aguilar*, 737 F.3d 251, 261 (2d Cir. 2013). However, the government did not rely upon settled precedent that happened to be reversed subsequently, which is where good faith intervenes. *See Davis v. United States*, 564 U.S. 229, 239 (2011) (noting compliance with Circuit law that was “then-binding”). Instead, when the government acted here, *Jones* had already been decided and “the decisions in this District and the Eastern District of New York [remained] split as to whether police need[ed] a search warrant for cell site location information.” *See, e.g., Cucuta v. New York City*, 25 F. Supp.3d 400, 416 (S.D.N.Y. 2014) (collecting cases).

In the shadow of this legal background, nothing would have stopped the government from erring on the side of caution and trying to obtain a search warrant before obtaining eighteen months’ worth of Tartaglione’s location-data. But the government took a more aggressive approach—betting on one side of the legal controversy, and retrieving the CSLI while spurning the warrant procedure altogether.

The exclusionary rule is thus appropriate, because it will “appreciabl[y] deter[]”⁹ the government from exploiting legal splits when more constitutionally conservative tactics remain available.

Nevertheless, the Second Circuit has thus far declined to impose the exclusionary rule for Fourth Amendment violations pre-*Carpenter*. In *United States v. Zodhiates*, 901 F.3d 137, 143-44 (2d Cir. 2018), the Circuit found a good-faith bridge over Fourth Amendment waters by using the third party doctrine. And in *United States v. Chambers*, 751 F. Appx 44, 46-47 (2d Cir. 2018), the Circuit extended *Zodhiates* even over cases decided after *Jones*. While this Court is, concededly, bound by *this facet* of the analysis in *Chambers* and *Zodhiates*, these decisions are wrongly decided and should ultimately be reversed. In the face of a raging legal controversy over the meaning of a statute and its related Fourth Amendment implications, and where a majority of the Supreme Court had already signaled its disapproval of the tactic in issue, “good faith” does not allow the government to bet on one side of the equation and to then obtain a heads-the-government wins, tails-the-defense loses outcome. The government can take the constitutionally modest approach and get a warrant, or can place a wager on one side of the legal split and bear the consequences if proven wrong.

Because the government violated Mr. Tartaglione’s rights under the Fourth Amendment when it obtained his CSLI without a warrant, and because it could not rely upon statutory law or settled Fourth Amendment jurisprudence to support these tactics, the CSLI records should be suppressed.

⁹ *Herring v. U.S.*, 555 U.S. 135, 141 (2009).

CONCLUSION

For these reasons, we respectfully request that the application to suppress the CSLI records of the defendant be GRANTED.

Dated: Garden City, New York
August 1, 2019

Respectfully,

BARKET EPSTEIN KEARON
ALDEA & LOTURCO, LLP

/s/Bruce Barket
Bruce Barket, Esq.
Aida Leisenring, Esq.
Alexander Klein, Esq.